Hiroshima Math. J., **54** (2024), 37–43
doi:10.32917/h2022004

Galois points and rational functions with small value sets

Dedicated to Professor Shun-ichi Kimura on the occasion of his 60th birthday

Satoru Fukasawa

(Received January 31, 2022)
(Revised February 27, 2023)

Abstract. This paper presents a connection between Galois points and rational functions with small value sets over a finite field. This paper proves that a defining polynomial of any plane curve admitting two Galois points is an irreducible factor of a polynomial obtained from the equality of two rational functions in one variable for each. Under the assumption that Galois groups of two Galois points generate their semidirect product, a recent result of Bartoli, Borges, and Quoos indicates that one of these rational functions over a finite field has a very small value set. This paper shows that when two Galois points are external, the defining polynomial is an irreducible factor of the difference of two polynomials in one variable. This connects the study of Galois points to that of polynomials with small value sets.

1. Introduction

This paper presents a connection between Galois points and rational functions with small value sets over a finite field.

Let $C \subset \mathbb{P}^2$ be an irreducible plane curve of degree $d > 1$ over an algebraically closed field k of characteristic $p \geq 0$ and let $k(C)$ be its function field. Taking a point $P \in \mathbb{P}^2$, we consider the projection $\pi_P : C \dashrightarrow \mathbb{P}^1$ from P. A point $P \in \mathbb{P}^2$ is called a *Galois point* if the field extension $k(C)/\pi_P^* k(\mathbb{P}^1)$ of function fields induced by π_P is a Galois extension ([5, 10, 13]). The associated Galois group is denoted by G_P. Numerous results on Galois points have been obtained; however, there are several open problems (see [5, 14]).

The author and Speziali examined plane curves with two outer Galois points $P_1, P_2 \in \mathbb{P}^2 \setminus C$ such that $\langle G_{P_1}, G_{P_2} \rangle = G_{P_1} \rtimes G_{P_2}$ ([7]), and the author examined plane curves admitting an inner Galois point $P_1 \in C \setminus \mathrm{Sing}(C)$ and an

The author was partially supported by JSPS KAKENHI Grant Number JP19K03438.

2020 *Mathematics Subject Classification*. Primary 14H05; Secondary 11T06.

Key words and phrases. Galois point, plane curve, finite field, rational function, value set.

outer Galois point $P_2 \in \mathbb{P}^2 \setminus C$ such that $\langle G_{P_1}, G_{P_2} \rangle = G_{P_1} \rtimes G_{P_2}$ or $G_{P_1} \ltimes G_{P_2}$ ([6]). In a more general situation, this paper proves the following.

Theorem. *Let $C \subset \mathbb{P}^2$ be defined over a finite field $\mathbb{F}_q$ of q elements. Assume that C is irreducible over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. Let $P_1 = (1:0:0), P_2 = (0:1:0) \in \mathbb{P}^2$. If P_1 and P_2 are Galois points such that all automorphisms in $G_{P_1} \cup G_{P_2}$ are defined over $\mathbb{F}_q$, and $|\langle G_{P_1}, G_{P_2} \rangle| < \infty$, then the following holds.*

(I) *There exist polynomials $f_1, g_1, f_2, g_2 \in \mathbb{F}_q[x]$ such that*

(a) *f_i and g_i are relatively prime for $i = 1, 2$,*

(b) $\max\{\deg f_i, \deg g_i\} = |\langle G_{P_1}, G_{P_2} \rangle| / |G_{P_j}|$ *for i, j with* $\{i, j\} = \{1, 2\}$,

(c) *the defining polynomial of C in the affine plane is an irreducible factor of*

$$f_1(x)g_2(y) - g_1(x)f_2(y)$$

over $\mathbb{F}_q$,

(d) $\mathbb{F}_q(f_1(x)/g_1(x)) = \mathbb{F}_q(f_2(y)/g_2(y)) = \mathbb{F}_q(C)^{\langle G_{P_1}, G_{P_2} \rangle}$.

Let $f_1, g_1, f_2, g_2 \in \mathbb{F}_q[x]$ be polynomials with conditions (a), (b), (c), *and* (d) *in* (I). *Then the following hold.*

(II) $|\langle G_{P_1}, G_{P_2} \rangle| = |G_{P_1}| \times |G_{P_2}|$ *if and only if the curve C is defined by*

$$f_1(x)g_2(y) - g_1(x)f_2(y) = 0.$$

(III) $\langle G_{P_1}, G_{P_2} \rangle = G_{P_1} \rtimes G_{P_2}$ *if and only if $\mathbb{F}_q(y)/\mathbb{F}_q(h_2(y))$ is a Galois extension for $h_2(y) = f_2(y)/g_2(y)$.*

(IV) *Assume that $P_1, P_2 \in \mathbb{P}^2 \setminus C$. Then we can take $g_1(x) = g_2(x) = 1$, namely, a defining polynomial of C is an irreducible factor of $f_1(x) - f_2(y)$ over $\mathbb{F}_q$. In this case, $|\langle G_{P_1}, G_{P_2} \rangle| = d^2$ if and only if $f_1(x) - f_2(y)$ is a defining polynomial.*

Remark 1. (a) *Theorem holds for any perfect field k_0, by replacing $\mathbb{F}_q$ by k_0.*

(b) *In assertion* (II), *we can always replace f_1 and g_1 so that* $\deg f_1 \neq \deg g_1$, *since if* $\deg f_1 = \deg g_1$, *then* $f_1/g_1 = \alpha + f_{11}/g_1$ *and* $\mathbb{F}_q(f_1/g_1) = \mathbb{F}_q(f_{11}/g_1)$ *for some $\alpha \in \mathbb{F}_q$ and $f_{11} \in \mathbb{F}_q[x]$ with* $\deg f_{11} < \deg g_1$.

(c) *Galois points are defined over algebraically closed fields. Theorem indicates that it is appropriate to define a Galois point P over a finite field $\mathbb{F}_q$ as an $\mathbb{F}_q$-rational point of $\mathbb{P}^2$ such that the extension $\mathbb{F}_q(C)/\mathbb{F}_q(L_1/L_2)$ is Galois, where $L_1, L_2 \in \mathbb{F}_q[X, Y, Z]$ are linearly independent homogeneous polynomials of degree one defining P.*

What are these rational functions f_1/g_1 and f_2/g_2? In a recent study [1], Bartoli, Borges, and Quoos examined rational functions $h(x) \in \mathbb{F}_q(x)$ with small value sets, and obtained the following theorem.

Fact (Bartoli, Borges, and Quoos). *Let $f(x), g(x) \in \mathbb{F}_q[x]$ be relatively prime. If a rational function $h(x) = f(x)/g(x) \in \mathbb{F}_q(x)$ is such that $\mathbb{F}_q(x)/\mathbb{F}_q(h(x))$ is a Galois extension, then either*

$$\#V_h = \left\lceil \frac{q+1}{\deg h} \right\rceil \qquad or \qquad \#V_h = \left\lceil \frac{q+1}{\deg h} \right\rceil + 1,$$

where $V_h = \{h(\alpha) \mid \alpha \in \mathbb{P}^1(\mathbb{F}_q)\} \subset \mathbb{P}^1(\mathbb{F}_q)$ and $\deg h = \max\{\deg f, \deg g\}$.

Theorem and Fact indicate that the rational function $h_2(y)$ as in Theorem (III) has a very small value set. More precisely:

Corollary 1. *Let $f_2(x), g_2(x) \in \mathbb{F}_q[x]$ be as in Theorem and let $h_2(x) = f_2(x)/g_2(x)$. If $\langle G_{P_1}, G_{P_2} \rangle = G_{P_1} \rtimes G_{P_2}$, then either*

$$\#V_{h_2} = \left\lceil \frac{q+1}{\deg h_2} \right\rceil \qquad or \qquad \#V_{h_2} = \left\lceil \frac{q+1}{\deg h_2} \right\rceil + 1.$$

Theorem (IV) connects the study of Galois points to that of polynomials over finite fields. Borges [2] developed a connection between minimal value set polynomials ([4, 9]) and Frobenius nonclassical curves ([8, 12]). Borges' theorem [2, Corollary 3.5] indicates the following.

Corollary 2. *Assume that $P_1, P_2 \in \mathbb{P}^2 \setminus C$. Let $f_1(x), f_2(x) \in \mathbb{F}_q[x]$ be polynomials as in Theorem and let V'_{f_1}, V'_{f_2} be their value sets, that is, $V'_{f_i} = \{f_i(\alpha) \mid \alpha \in \mathbb{F}_q\}$ for $i = 1, 2$. If f_1, f_2 are minimal value set polynomials such that $V'_{f_1} = V'_{f_2}$ and either $|V'_{f_1}| > 2$ or $|V'_{f_1}| = 2 = p$, then C is q-Frobenius nonclassical.*

The Fermat curve

$$x^{(q-1)/(q'-1)} + y^{(q-1)/(q'-1)} + 1 = 0$$

with $\mathbb{F}_{q'} \subset \mathbb{F}_q$ is a typical example of a curve that satisfies the assumptions in Corollary 2. Points $(1:0:0)$, $(0:1:0)$ are outer Galois points ([5, 10, 13]), and polynomials $x^{(q-1)/(q'-1)}$ and $-y^{(q-1)/(q'-1)} - 1$ have the same minimal value set $\mathbb{F}_{q'}$ ([2]). Another example is found in [3, Theorem 2].

Remark 2. *Assume that $f(x) \in \mathbb{F}_q[x]$ and a field extension $\mathbb{F}_q(x)/\mathbb{F}_q(f(x))$ is Galois. A place at infinity is a total ramification point and there exist at most two short orbits. An approach similar to the proof of Fact (see* [1, Proof of Theorem 2.1]*) can be used to confirm that $f(x)$ is a minimal value set polynomial.*

2. Proofs

PROOF (Proof of Theorem). Assume that points $P_1 = (1:0:0), P_2 = (0:1:0) \in \mathbb{P}^2$ are Galois points, and that the group $G := \langle G_{P_1}, G_{P_2} \rangle$ is of finite order. The projections π_{P_1} and π_{P_2} from points P_1 and P_2 are represented by

$$\pi_{P_1}(x, y) = y \qquad \text{and} \qquad \pi_{P_2}(x, y) = x$$

respectively. Since all elements of $G_{P_1} \cup G_{P_2}$ are defined over $\mathbb{F}_q$ and the defining polynomial of C over $\mathbb{F}_q$ is irreducible over $\overline{\mathbb{F}}_q$, it follows that $\mathbb{F}_q(C)^{G_{P_1}} = \mathbb{F}_q(y)$ and $\mathbb{F}_q(C)^{G_{P_2}} = \mathbb{F}_q(x)$. Since $|G| < \infty$, by Lüroth's theorem, there exists a function $t \in \mathbb{F}_q(C)^G$ such that $\mathbb{F}_q(t) = \mathbb{F}_q(C)^G$. Since $\mathbb{F}_q(t) \subset \mathbb{F}_q(y)$ and $\mathbb{F}_q(t) \subset \mathbb{F}_q(x)$, there exist polynomials $f_2(y), g_2(y) \in \mathbb{F}_q[y]$ and $f_1(x), g_1(x) \in \mathbb{F}_q[x]$ such that

$$t = f_2(y)/g_2(y) \qquad \text{and} \qquad t = f_1(x)/g_1(x).$$

We can assume that polynomials $f_i(x)$ and $g_i(x)$ are relatively prime for $i = 1, 2$. Let $h_i(x) = f_i(x)/g_i(x)$ for $i = 1, 2$. Since

$$\mathbb{F}_q(y)/\mathbb{F}_q(h_2(y)) = \mathbb{F}_q(C)^{G_{P_1}}/\mathbb{F}_q(C)^G,$$

$$\mathbb{F}_q(x)/\mathbb{F}_q(h_1(x)) = \mathbb{F}_q(C)^{G_{P_2}}/\mathbb{F}_q(C)^G,$$

it follows that

$$\max\{\deg f_2, \deg g_2\} = |G|/|G_{P_1}|, \qquad \max\{\deg f_1, \deg g_1\} = |G|/|G_{P_2}|.$$

Since $f_1(x)/g_1(x) = t = f_2(y)/g_2(y)$ in $\mathbb{F}_q(C)$, it follows that

$$f(x, y) := f_1(x)g_2(y) - g_1(x)f_2(y) = 0$$

in $\mathbb{F}_q(C)$. Assertion (I) follows.

Let $f_1, g_1, f_2, g_2 \in \mathbb{F}_q[x]$ be polynomials with conditions (a), (b), (c), and (d) in (I). Assume that $|G| = |G_{P_1}| \times |G_{P_2}|$. Note that

$$|G_{P_1}| = |G|/|G_{P_2}| = \max\{\deg f_1, \deg g_1\}.$$

Since

$$\deg_x f(x, y) \le \max\{\deg f_1(x), \deg g_1(x)\} = |G_{P_1}| = \deg \pi_{P_1},$$

it follows that $\deg_x f(x, y) = \deg \pi_{P_1}$ and $f(x, y)$ is a minimal polynomial of x over $\overline{\mathbb{F}}_q(y)$. This indicates that $f(x, y)$ is irreducible as an element of $\overline{\mathbb{F}}_q(y)[x]$. Thus, $f(x, y)$ is irreducible in $\overline{\mathbb{F}}_q[x, y]$.

Assume that $f(x, y)$ is a defining polynomial of C. Note that if $\alpha \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_q$ are the leading coefficients of $f_1(x)$ and of $g_1(x)$ respectively, then the leading coefficient of $f(x, y)$ as an element of $(\mathbb{F}_q(y))[x]$ is $\alpha g_2(y)$, $-\beta f_2(y)$, or $\alpha g_2(y) - \beta f_2(y)$. Then

$$\max\{\deg f_1, \deg g_1\} = \deg_x f(x, y) = \deg \pi_{P_1} = |G_{P_1}|.$$

Since $|G|/|G_{P_2}| = \max\{\deg f_1, \deg g_1\}$, it follows that

$$|G| = |G_{P_1}| \times |G_{P_2}|.$$

Assertion (II) follows.

$G = G_{P_1} \rtimes G_{P_2}$ if and only if G_{P_1} is a normal subgroup of G. Assertion (III) follows, by Galois theory.

Assume that $P_1, P_2 \in \mathbb{P}^2 \setminus C$. Let $\varphi_i : \mathbb{P}^1 \to \mathbb{P}^1$ be the morphism corresponding to $\overline{\mathbb{F}}_q(C)^{G_{P_i}}/\overline{\mathbb{F}}_q(C)^G$ for $i = 1, 2$. Let Q be a place of $\overline{\mathbb{F}}_q(C)$ coming from $C \cap \overline{P_1P_2}$, where $\overline{P_1P_2}$ is a line passing through P_1 and P_2. Since the fiber of $\varphi_i(\pi_{P_i}(Q))$ for the covering $\varphi_i \circ \pi_{P_i}$ coincides with the orbit $G \cdot Q$ (see [11, III.7.1]), it follows that

$$\varphi_i^{-1}(\varphi_i(\pi_{P_i}(Q))) = \pi_{P_i}(G \cdot Q),$$

for $i = 1, 2$. Since $P_1, P_2 \in \mathbb{P}^2 \setminus C$, it follows that

$$\pi_{P_i}(G \cdot Q) = \{\pi_{P_i}(Q)\},$$

and that φ_i is totally ramified at $\pi_{P_i}(Q)$, for $i = 1, 2$. We take a system $(Y : Z)$ of coordinates on $\pi_{P_1}(C) \cong \mathbb{P}^1$ (resp. a system $(X : Z)$ of coordinates on $\pi_{P_2}(C) \cong \mathbb{P}^1$) such that $\pi_{P_1}(Q) = (1 : 0)$ (resp. $\pi_{P_2}(Q) = (1 : 0)$). Note that

$$\varphi_1(\pi_{P_1}(Q)) = \varphi_2(\pi_{P_2}(Q)).$$

We consider a system $(t : 1)$ of coordinates on $\varphi_1(\pi_{P_1}(C)) = \varphi_2(\pi_{P_2}(C)) \cong \mathbb{P}^1$ such that

$$\varphi_1(\pi_{P_1}(Q)) = (1 : 0) = \varphi_2(\pi_{P_2}(Q)).$$

Since φ_1 (resp. φ_2) is totally ramified at $(1 : 0)$ and $\varphi_1(1 : 0) = (1 : 0)$ (resp. $\varphi_2(1 : 0) = (1 : 0)$), it follows that $\varphi_1(y : 1) = (f_2(y) : 1)$ (resp. $\varphi_2(x : 1) = f_1(x)$) for some polynomial $f_2(y) \in \mathbb{F}_q[y]$ (resp. $f_1(x) \in \mathbb{F}_q[x]$). Since $f_2(y) = t = f_1(x)$ in $\mathbb{F}_q(C)$, the former assertion of (IV) follows. The latter assertion of (IV) comes from assertion (II). □

Corollary 2 is derived from Borges' theorem [2, Corollary 3.5]. In [2, Theorem 3.4, Corollary 3.5], it is assumed that *all* irreducible factors of $f(x) - g(y)$ are defined over $\mathbb{F}_q$. Therefore, we confirm that the reasoning in Borges' study [2] can be applied to our case, and that any factor of $f_1(x) - f_2(y)$ defined over $\mathbb{F}_q$ is q-Frobenius nonclassical, under the assumption on f_1, f_2 as in Corollary 2.

Proof (Proof of Corollary 2). Let $P_1, P_2 \in \mathbb{P}^2 \setminus C$, and let $f_1, f_2 \in \mathbb{F}_q[x]$ be polynomials as in Theorem. Assume that f_1, f_2 are minimal value set polynomials such that $V'_{f_1} = V'_{f_2}$ and either $|V'_{f_1}| > 2$ or $|V'_{f_1}| = 2 = p$. By [2, Theorem 2.2], there exist $\theta_i \in \mathbb{F}_q^*$ and a monic polynomial $T_i = \prod_{\gamma \in V'_{f_i}} (x - \gamma) \in \mathbb{F}_q[x]$ such that

$$T_i(f_i) = \theta_i (x^q - x) f_{i,x}$$

for $i = 1, 2$, where $f_{i,x}$ is the formal derivative of f_i by x. Since $V'_{f_1} = V'_{f_2}$, it follows that $T_1 = T_2$. By [2, Lemma 2.4 (ii)], $\theta_1 = \theta_2$. Since $X - Y$ divides $T_1(X) - T_1(Y)$, it follows that $f(x, y) = f_1(x) - f_2(y)$ divides

$$(x^q - x) f_x + (y^q - y) f_y = (x^q - x) f_{1,x} - (y^q - y) f_{2,y}.$$

Since the defining polynomial f_0 of C is an irreducible factor of $f(x, y)$, it follows from [2, Lemma 3.2] and [2, Lemma 3.3 (i) $\Rightarrow$ (ii)] that f_0 divides

$$(x^q - x) f_{0,x} + (y^q - y) f_{0,y},$$

that is, C is q-Frobenius nonclassical. $\square$

Acknowledgements

The author is grateful to Doctor Kazuki Higashine for the helpful discussions during this study. The author thanks Professor Nobuyoshi Takahashi for helpful comments, which improved assertion (II) in Theorem.

References

[1] D. Bartoli, H. Borges, and L. Quoos, Rational functions with small value set, J. Algebra **565** (2021), 675–690.

[2] H. Borges, Frobenius nonclassical components of curves with separated variables, J. Number Theory **159** (2016), 402–425.

[3] H. Borges and S. Fukasawa, An elementary abelian p-cover of the Hermitian curve with many automorphisms, Math. Z. **302** (2022), 695–706.

[4] L. Carlitz, D. J. Lewis, W. H. Mills, and E. G. Straus, Polynomials over finite fields with minimal value sets, Mathematika **8** (1961), 121–130.

[5] S. Fukasawa, Galois points for a plane curve in arbitrary characteristic, Geom. Dedicata **139** (2009), 211–218.

[6] S. Fukasawa, Algebraic curves admitting inner and outer Galois points, preprint, arXiv:2010.00815.

[7] S. Fukasawa and P. Speziali, Plane curves possessing two outer Galois points, preprint, arXiv:1801.03198.

[8] A. Hefez and J. F. Voloch, Frobenius non classical curves, Arch. Math. **54** (1990), 263–273.

[9] W. H. Mills, Polynomials with minimal value sets, Pacific J. Math. **14** (1964), 225–241.

[10] K. Miura and H. Yoshihara, Field theory for function fields of plane quartic curves, J. Algebra **226** (2000), 283–294.

[11] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer-Verlag, Berlin, 1993.

[12] K.-O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields, Proc. Lond. Math. Soc. (3) **52** (1986), 1–19.

[13] H. Yoshihara, Function field theory of plane curves by dual curves, J. Algebra **239** (2001), 340–355.

[14] H. Yoshihara and S. Fukasawa, List of problems, https://sites.google.com/sci.kj.yamagata-u.ac.jp/fukasawa-lab/open-questions-english

Satoru Fukasawa
Faculty of Science
Yamagata University
Yamagata 990-8560 *JAPAN*
E-mail: s.fukasawa@sci.kj.yamagata-u.ac.jp